

AMANDA GRIER
COLLEEN B. ROBBINS
ELSIE B. KAPPLER
FEDERAL TRADE COMMISSION
(Each appearing pursuant to DUCivR83-1.1(e))
Attorneys for Plaintiff
Division of Marketing Practices
600 Pennsylvania Ave., N.W., CC-8528
Washington, DC 20580
Telephone: (202) 326-3745
agrier@ftc.gov
crobbins@ftc.gov
ekappler@ftc.gov

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH, CENTRAL DIVISION**

FEDERAL TRADE COMMISSION, and

Plaintiff,

v.

ELITE IT PARTNERS, INC., a Utah
corporation doing business as ELITE IT
HOME, and

JAMES MICHAEL MARTINOS,
individually and as an officer of ELITE IT
PARTNERS, INC.,

Defendants.

Case No. 2:19cv125

**FILED UNDER SEAL
PURSUANT TO COURT
ORDER
(DOCKET NO. _____)**

**COMPLAINT FOR
PERMANENT INJUNCTION
AND OTHER EQUITABLE
RELIEF**

Plaintiff, the Federal Trade Commission (“FTC”) for its Complaint alleges:

1. The FTC brings this action under Sections 13(b) and 19 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 53(b) and 57b, the Telemarketing and Consumer Fraud and Abuse Prevention Act (“Telemarketing Act”), 15 U.S.C. §§ 6101-6108, as amended,

and Section 5 of the Restore Online Shoppers' Confidence Act ("ROSCA"), 15 U.S.C. §§ 8401-8405, to obtain temporary, preliminary, and permanent injunctive relief, rescission or reformation of contracts, restitution, the refund of monies paid, disgorgement of ill-gotten monies, and other equitable relief for Defendants' acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), the FTC's Telemarketing Sales Rule ("TSR"), 16 C.F.R. Part 310, as amended, and Section 4 of ROSCA, 15 U.S.C. § 8403.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331, 1337(a), and 1345, and 15 U.S.C. §§ 45(a), 53(b), 57b, 6102(c), 6105(b), and 8404(a).

3. Venue is proper in this district under 28 U.S.C. § 1391(b)(1-3), (c)(1-2), and (d), and 15 U.S.C. § 53(b).

PLAINTIFFS

4. The FTC is an independent agency of the United States Government created by statute. 15 U.S.C. §§ 41-58. The FTC enforces Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits unfair or deceptive acts or practices in or affecting commerce.

5. The FTC also enforces the Telemarketing Act, 15 U.S.C. §§ 6101-6108, as amended. Pursuant to the Telemarketing Act, the FTC promulgated and enforces the TSR, 16 C.F.R. Part 310, which prohibits deceptive and abusive telemarketing acts or practices.

6. The FTC also enforces ROSCA, 15 U.S.C. §§ 8401-8405. ROSCA prohibits the sale of goods or services on the Internet through negative option marketing without meeting certain requirements to protect consumers. A negative option is an offer in which the seller treats a consumer's silence—their failure to reject an offer or cancel an agreement—as consent to be charged for goods or services.

7. The FTC is authorized to initiate federal district court proceedings, by its own attorneys, to enjoin violations of the FTC Act, TSR, and ROSCA, and to secure such equitable relief as may be appropriate in each case, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies. 15 U.S.C. §§ 53(b), 56(a)(2)(A)-(B), 57b, 6102(c), 6105(b), and 8404.

DEFENDANTS

8. Defendant Elite IT Partners, Inc. (“Elite”) is a Utah corporation with its principal place of business at 1548 North Technology Way, Building D, Suite 1100, Orem, Utah 84097. Elite transacts or has transacted business in this district and throughout the United States. At all times material to this Complaint, acting alone or in concert with others, Elite has advertised, marketed, distributed, or sold computer security or technical support services to consumers throughout the United States.

9. Defendant James Michael Martinos (“Martin”) is the President of Elite. At all times material to this Complaint, acting alone or in concert with others, he has formulated, directed, controlled, had the authority to control, or participated in the acts and practices of Elite set forth in this Complaint. Defendant Martinos resides in Midway, Utah, and, in connection with the matters alleged herein, transacts or has transacted business in this district and throughout the United States.

COMMERCE

10. At all times material to this Complaint, Defendants have maintained a substantial course of trade in or affecting commerce, as “commerce” is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

DEFENDANTS' BUSINESS ACTIVITIES

11. Since at least 2014, Defendants have been operating a technical support scheme that relies on both internet and telephone communication with consumers, including through outbound calls prompted by internet searches that lead consumers to Defendants' website. The vast majority of consumers Elite contacts are elderly and/or unfamiliar with the workings of computers or the internet. Defendants use intimidation and scare tactics to take advantage of these consumers' limited knowledge about such technology.

12. In numerous cases, consumers who interact with Elite are seeking assistance with password recovery for email and other accounts. Rather than provide the services requested by consumers, Defendants' salespeople insist on gaining access to consumers' computers to perform a sham "diagnostic." Defendants' representatives then falsely state to consumers that their computers are infected with viruses and infections that threaten the security of consumers' personal information and prevent consumers from accessing their email and other accounts. In numerous cases, Defendants misrepresent that consumers have inadequate or no antivirus protection. After making these misrepresentations, Defendants dupe many consumers into paying large sums for an immediate cleaning of their computers and ongoing computer technical support services.

13. Defendants fail to disclose, or to disclose adequately, material terms, including that consumers who sign up for ongoing technical services for a monthly rate are signed up for a full 12-month term that automatically renews for another year if the consumer fails to timely cancel; that to cancel services, the consumer must do so in writing at least 30 days before the end of the 12-month term; and that consumers who cancel services within the first 12 months will be subject to a \$150 cancellation fee. Many consumers never even obtain the services that

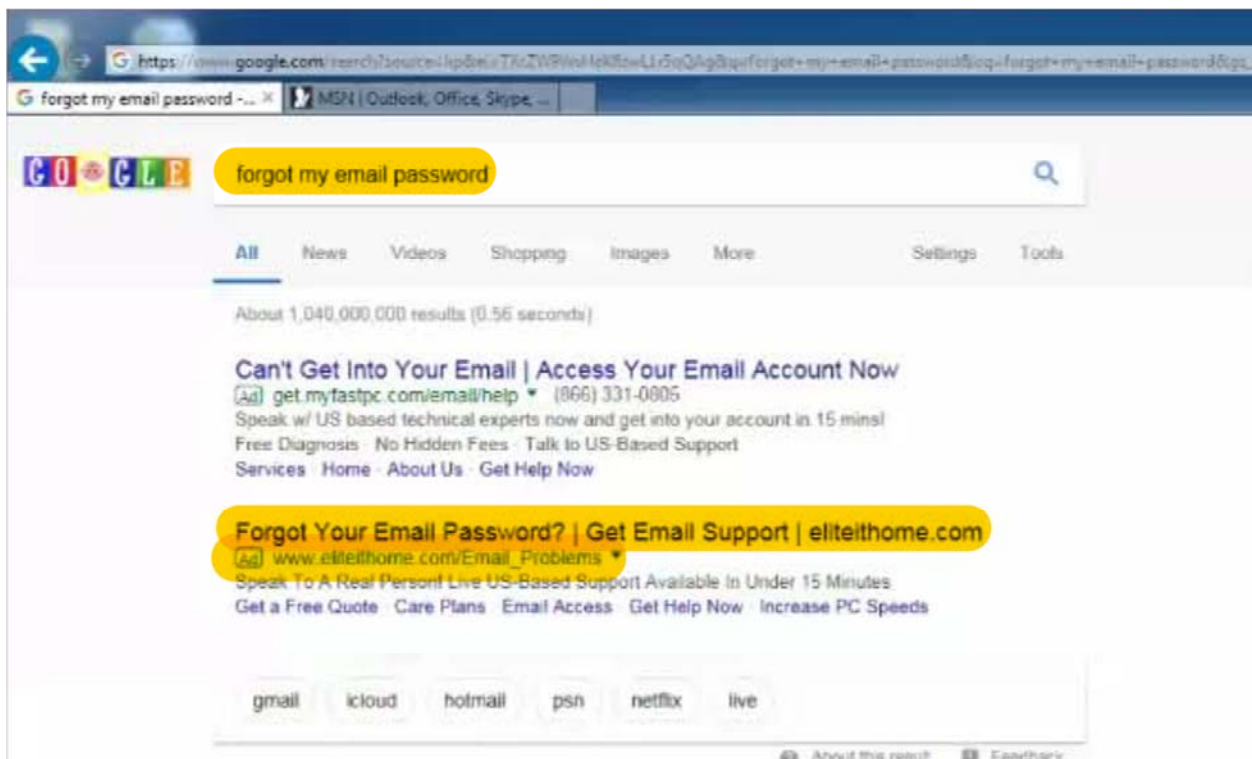
prompted them to contact the company initially, and discover that Defendants have deleted important programs or damaged their computers.

Defendants' Sales Practices

14. In some instances, Defendants place unsolicited calls to consumers to sell their services.

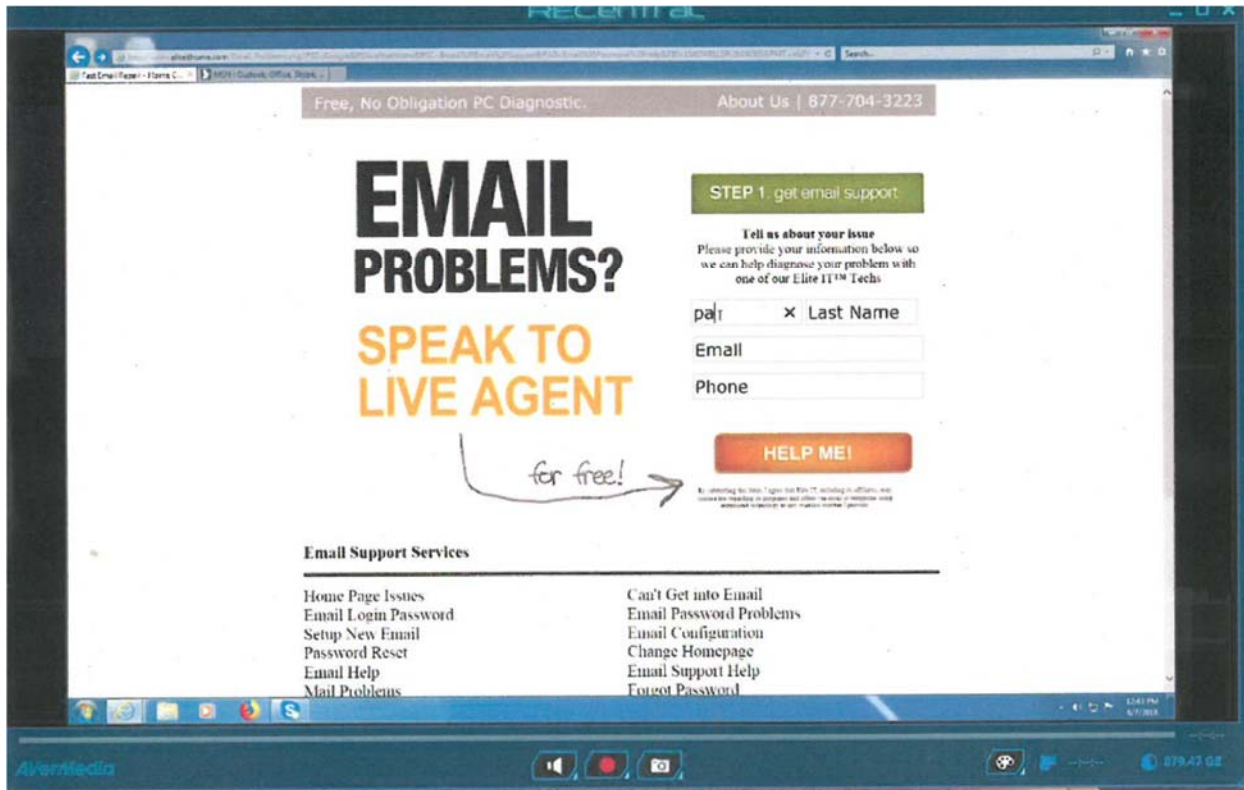
15. In other instances, Defendants attract consumers using search engine optimization tools such as "Google Adwords." Google Adwords is one of various paid services that drive consumers to particular websites based on key search terms. Among other things, Defendants' key search terms relate to consumers' inability to access email and other accounts because they have misplaced or forgotten their passwords. **Figure 1**, below, illustrates the search process and result, with the search terms and result highlighted.

Figure 1

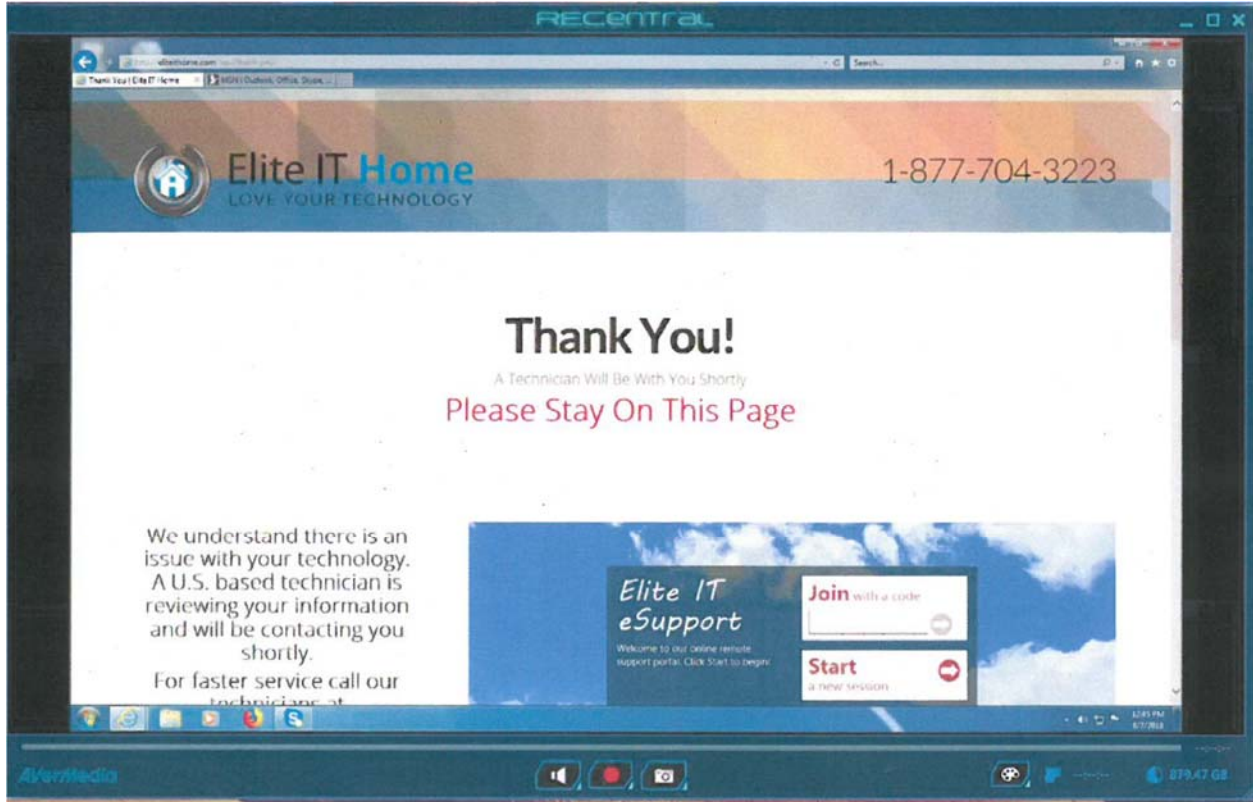


16. When consumers click on the sponsored result link for Elite, they are directed to a webpage for the company (www.eliteithome.com/Email_Problems) that offers a “free, No Obligation PC Diagnostic” for “Email Problems,” illustrated in **Figure 2**, below.

Figure 2



17. Once consumers land on Defendants’ webpage, Defendants invite them to “SPEAK TO A LIVE AGENT” by providing their name, email address, and phone number. Consumers who submit this information by pressing the “HELP ME!” button, are then directed to another webpage for Elite, pictured in **Figure 3**, below. Defendants then contact the consumers by telephone.

Figure 3

18. Paragraphs 19 through 40 describe Defendants' sales practices regardless of the initial contact method.

19. Defendants' salespeople state or imply, either directly, indirectly, or by failing to correct consumers' obvious misimpressions, that they are, or are authorized to provide services for, consumers' internet or email providers, or other large well-known companies. In numerous instances, Defendants' representatives falsely state that two internet service and email providers, AOL and Yahoo, are defunct and no longer provide customer service.

20. Regardless of the consumer's stated problem, Defendants' sales representatives are trained to tell the consumer that any problem is likely related to viruses and infections, and to insist that Elite must gain remote access to the consumer's computer to diagnose the problem.

21. To initiate a remote session and gain access to consumers' computers, Defendants' sales representatives direct consumers to a remote connection webpage run by LogMeIn. Once Defendants' sales representatives have access, consumers are able to see the sales representatives' activity on their computer screen. At this point, Defendants' sales representatives can completely control the consumers' computers and, for example, can move the cursor, "draw" on the screen, enter commands, run applications, and access stored information. Working from a script, Elite's salespeople then walk the consumer through a purported diagnostic process that inevitably leads to the conclusion that the consumer's computer is infected with viruses and infections and must be cleaned to ensure the security of the consumer's private information, including passwords, and allow for access to email and other accounts.

Defendants' "Diagnostic"

22. After gaining access to consumers' computers, Defendants' representatives' first step is to download and run a free version of a diagnostic tool available on the internet called "SUPERAntispyware." SUPERAntispyware purports to identify multiple "Detected Threats" as depicted in **Figure 4**, below. In numerous instances, these so-called "Detected Threats" are only "cookies." Cookies are small text files placed on a user's computer/browser when visiting certain websites. Web browsers use cookies to provide routine features for consumers, such as storing consumers' preferences. The Windows operating system is constantly creating temporary files as part of its normal behavior and these files do not constitute a problem, but are merely artifacts of normal system behavior that are always present in a computer running Microsoft Windows operating system. In addition, web-browsing cookies are almost always benign. Cookies cannot and do not: access or read a computer's hard drive, access a user's

personal information, or send emails or control functions on a user's computer. They are not "threats" in any sense.

Figure 4

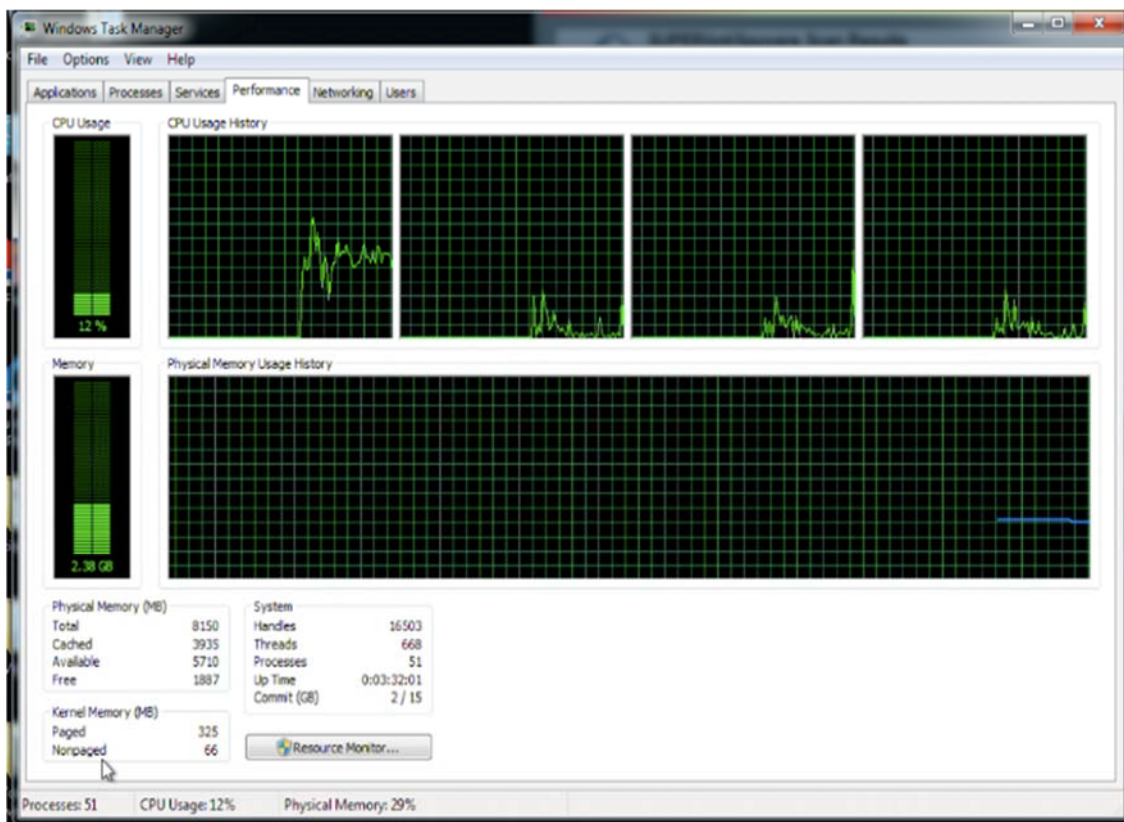


23. Defendants' salespeople, however, are instructed to tell consumers that the items detected, even if merely cookies, are dangerous and allow information to be stolen from the user's computer. They insist that the items must be removed, even when the consumer is only seeking assistance in recovering a password or accessing an account.

24. Another step in the “diagnostic” is for Defendants’ salespeople to open Windows “Task Manager,” and show consumers the information displayed about CPU (Central Processing Unit) usage and processes.

25. The salespeople tell consumers that the graph of CPU usage, as shown in **Figure 5**, below, indicates the existence of a virus when the CPU usage is high. While speaking to the sales representative, the consumer sees the CPU usage going up and down in the graph. Defendants’ salespeople tell the consumer that a high CPU usage is a “red flag” that indicates that the computer is working too hard.

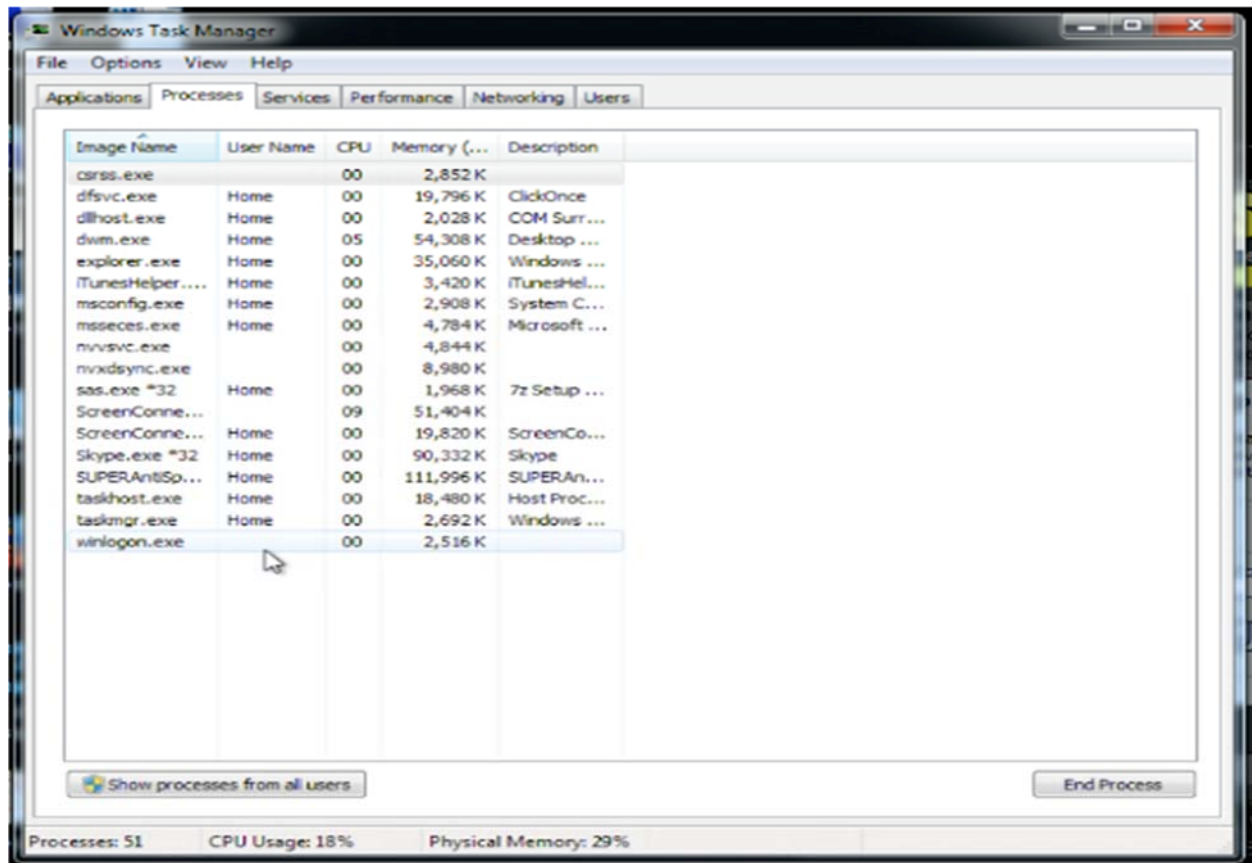
Figure 5



26. The representatives' statements are false. If a computer is managing a heavy workload, the CPU will constantly run higher with no adverse effects on the computer. The CPU is designed to run at maximum power for long periods of time.

27. Defendants' sales representatives also open the "processes" tab on Windows Task Manager, as depicted in **Figure 6**, below.

Figure 6

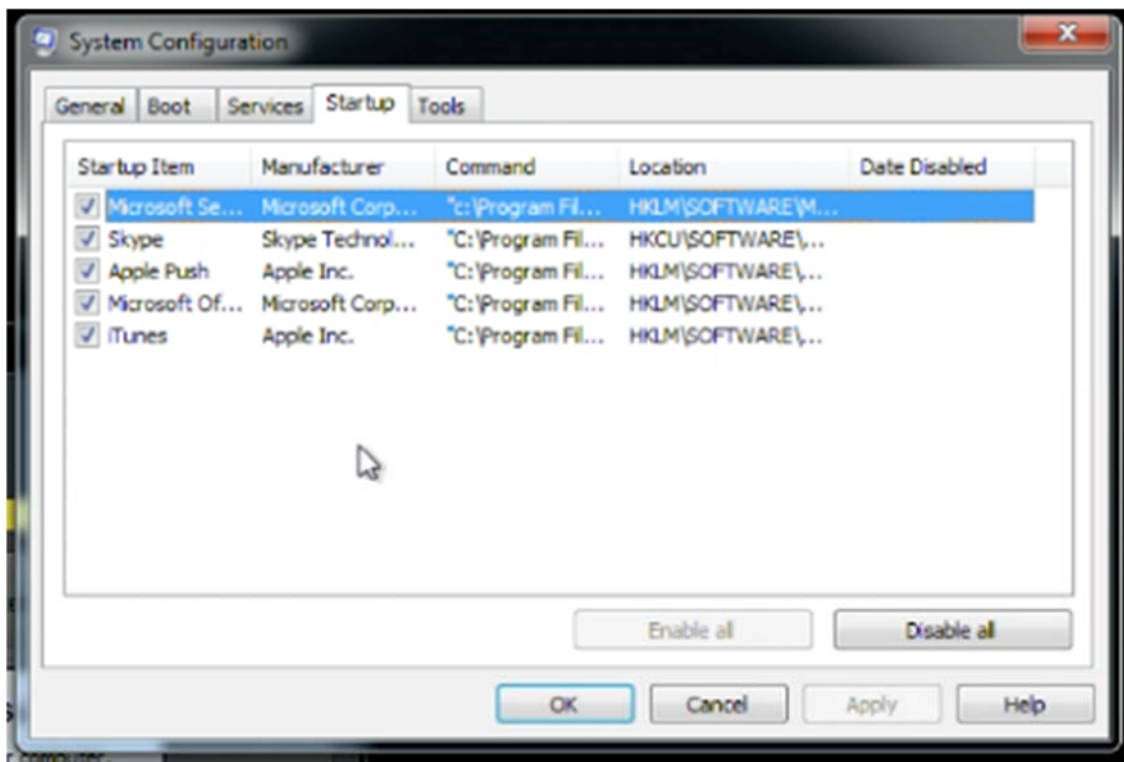


28. Defendants' representatives warn consumers that a large number of processes indicates the presence of malicious software and viruses. In fact, no one can detect the presence of malicious software and viruses merely by looking at the number of processes running. The representatives' statements are false.

29. Defendants' representatives also point to the absence of "user" names in the processes menu for some processes, telling consumers that this is a "red flag" or indication that the computer is infected. In fact, the absence of a "user name" value is typical, and does not indicate a problem on the system or the presence of a virus.

30. Defendants' salespeople also run the MSCONFIG.EXE application, which displays information on the start-up menu, as depicted in **Figure 7**, below.

Figure 7



31. Defendants' representatives tell consumers that if an antivirus program is installed and running properly, it should appear on the start-up menu, and that because no antivirus program appears in the start-up menu, the consumer's computer is exposed to viruses as there is no properly running antivirus program on the computer. This is false. The programs displayed on the start-up screen are those that are started when the user logs in. Antivirus software is

started shortly after the Windows operating system begins running and would not be displayed on this screen.

32. Defendants' salespeople use this portion of the diagnostic to pitch Elite's preferred antivirus program, "Trend Micro Pro," which they claim is distinct from other antivirus programs in that it runs continuously, while others allegedly scan only once a day. In fact, most antivirus software programs run continuously, including programs pre-loaded on Windows-based systems such as Microsoft Defender, and its earlier iteration, Microsoft Security Essentials.

33. By exploiting consumers' concerns about internet threats like viruses and other infections, and misrepresenting to consumers that they have no antivirus—or inadequate antivirus—protection, Defendants scare consumers into believing that their computers are in imminent danger. Based on Defendants' misrepresentations and unsubstantiated claims, Consumers spend \$99.99 or more for a one-time "cleaning" of non-existent viruses and infections from their computers.

34. Using the same misrepresentations and scare tactics, Defendants then upsell consumers additional technical support service plans that typically cost \$19.99 (Gold Care), \$29.99 (Platinum Care), and \$39.99 (Unlimited Care) per month, respectively. These plans are distinct from the one-time services provided by Elite because they also include what Defendants describe as "preventative care" services at increasing levels of frequency (Gold – every 90 days; Platinum – every 45 days; and Unlimited – unlimited technical support during business hours), antivirus software (Trend Micro Pro), data backup, help desk services, and data recovery. After Defendants have enrolled consumers in technical support service plans, they further upsell their higher grade plans.

35. Defendants fail to disclose orally prior to obtaining consumers' consent to payment, the terms of enrollment in its technical support service plans, including that they require a one-year commitment, and that the plans automatically renew—and the consumer is charged—for a second year if he or she fails to cancel in writing at least 30 days prior to the end of the year.

36. Defendants also fail to disclose orally prior to obtaining consumers' consent to payment, that consumers who cancel within the first year will be charged a \$150 early cancellation fee. They also fail to disclose orally to consumers who upgrade their technical support service plans that the one-year commitment restarts with the upgrade.

37. As illustrated in the screen shot in **Figure 8**, below, consumers are required to submit their payment information without Elite clearly and conspicuously disclosing on the consumer's computer screen all material terms of the transactions referred to in Paragraphs 35 and 36. Instead, this information is buried in terms and conditions that do not appear on the sign-up page.

Figure 8

Elite IT Home
LOVE YOUR TECHNOLOGY

You have selected our Gold Plan!

Payment Type:

Name on Card:

Card Number:

Expiration Date:

CVV:

Address:

Address(Cont):

City:

Country:

State/Prov:

Postal Code:

Please read the Terms and Conditions [Here](#)

Click here to accept the Terms and Conditions: ☐

Proceed →

LifeLock LifeLock Certified Partner

Devices Covered: Subscription Amount: \$19.99
Billing Cycle: Billing Date:

Repairs:

sh: 2018-06-07 13:39
HAS 53 PROGRAMS
KEY STROKING
RESEARCH / EMAIL / SHOPPING ONLINE AMAZON

Total Cost: 169.97

38. Defendants not only fail to disclose orally and visually on the consumer's computer screen material terms and conditions of their technical support service plans prior to obtaining payment, but also impose a burdensome cancellation procedure, which requires consumers to send a written letter at least 30 days prior to the expiration of the year term.

39. After consumers have paid Elite for a one-time cleaning or enrolled in a technical support service plan, Defendants then typically disclose orally their terms and conditions and send an email confirming the payment. A partial list of the terms and conditions of Defendants' services referenced in Paragraphs 35 and 36 are in small hard-to-read print at the bottom of the second page of the email. In numerous cases, Elite sends these emails to email addresses that Elite knows the consumer is unable to access. Indeed, the consumers' lack of access to their email address is often the primary reason for the purchase.

40. Many consumers are unaware that they have been enrolled in a technical support service plan, let alone such a service plan that requires a year's commitment and that automatically renews if the consumer does not cancel by written letter 30 days before the end of one year. Consumers who do realize they are being charged a monthly fee, or who elect to stop Defendants' services because they find them unhelpful or harmful, are then shocked by Defendants' insistence that they pay a \$150 cancellation fee. In numerous cases, Defendants refuse to honor consumers' cancellation requests. Defendants also threaten consumers who stop paying with collection actions.

Defendants' "Cleanings"

41. After convincing consumers to purchase their services, Defendants' telemarketers then transfer the consumer's remote access session to a purported technician to perform "cleanings." The cleanings consist of running free versions of software such as Malwarebytes and CCleaner, removing harmless temporary internet files, and disabling start-up programs such as Skype and iTunes helper.

42. Defendants sometimes uninstall consumers' antivirus and other programs without consumers' consent. In some instances, Defendants' technicians cause actual damage by deleting important files and programs, and compromise consumers' security by leaving them without proper antivirus protection. In addition to the substantial amount of money consumers pay for Defendants' services, many consumers have had to pay outside third-parties to repair damage done to their computers or have lost the use of their computers entirely.

The Role of Individual Defendant James Martinos

43. James Martinos is the founder, President, and Chief Executive Officer of Elite. He is the officer of record on Elite's filings with the Utah Secretary of State. Martinos is also the

authorized signer for Elite's business account with Wells Fargo Bank, N.A. He is the registrant for numerous websites used by Elite in the course of its business, including eliteitpartners.com, eliteithome.com, and eliteitbusiness.com. Martinos signed the contract with Elite's payment processor from November 2011 to August 2018, and has been a primary point of contact with this payment processor regarding chargebacks requested by consumers. In September 2018, he opened a merchant account for Elite with a new payment processor and was responsible for migrating Elite's business to the new processor. Martinos also received and responded to consumer complaints sent to him by the Utah Division of Consumer Protection.

VIOLATIONS OF SECTION 5 OF THE FTC ACT

44. Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), prohibits "unfair or deceptive acts or practices in or affecting commerce."

45. Misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices prohibited by Section 5(a) of the FTC Act.

COUNT I Deceptive Representations About Viruses and Infections

46. In numerous instances, in the course of marketing, offering for sale, and selling technical support services, Defendants represent or have represented, expressly or by implication, through a variety of means, including through telephone calls and Internet communications, that they have detected viruses and infections on consumers' computers that affect the security of consumers' computers and prevent access to consumers' email and other accounts.

47. In truth and in fact, in numerous instances in which Defendants have made the representations set forth in Paragraph 46, Defendants have not detected viruses and infections on

consumers' computers that affect the security of consumers' computers and prevent access to consumers' email and other accounts.

48. Therefore, Defendants' representations as set forth in Paragraph 46 are false, misleading, or were not substantiated at the time they were made, and thus, they constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT II

Deceptive Misrepresentations About Affiliations

49. In numerous instances, in connection with the marketing, offering for sale, or selling of technical support services, Defendants represent or have represented, directly or indirectly, expressly or by implication, through a variety of means, including telephone calls and internet communications, that they are part of, affiliated with, or authorized to provide services for well-known U.S. technology companies.

50. In truth and in fact, Defendants are not part of, affiliated with, or authorized to provide services for well-known U.S. technology companies.

51. Therefore, Defendants' representations as set forth in Paragraph 49 of this Complaint are false or misleading and constitute deceptive acts or practices in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

VIOLATIONS OF THE TELEMARKETING SALES RULE

52. Congress directed the FTC to prescribe rules prohibiting abusive and deceptive telemarketing acts or practices pursuant to the Telemarketing Act, 15 U.S.C. §§ 6101-6108, in 1994. The FTC adopted the original Telemarketing Sales Rule in 1995, extensively amended it in 2003, and amended certain provisions thereafter.

53. Defendants are "seller[s]" and/or "telemarketer[s]" engaged in "telemarketing, and Defendants have initiated, or caused telemarketers to initiate, "outbound telephone call[s]" to

consumers to induce the purchase of goods or services, as those terms are defined in the TSR, 16 C.F.R. § 310.2(v), (aa), (cc), and (dd).

54. Under the TSR, an “outbound telephone call” means “a telephone call initiated by a telemarketer to induce the purchase of goods or services or to solicit a charitable contribution.” 16 C.F.R. § 310.2(x).

55. The TSR prohibits telemarketers from “[m]aking . . . false or misleading statement[s] to induce any person to pay for goods or services or to induce a charitable contribution.” 16 C.F.R. § 310.3(a)(4).

56. The TSR’s prohibition against making false or misleading statements applies to all statements regarding upsells, whether the statements were made during an outbound call initiated by the telemarketer or an inbound call initiated by a consumer. 16 C.F.R. § 310.6(b)(4) and 310.6(b)(5)(iii).

57. Defendants’ offers include offers of technical support services with negative options features. Section 310.2(w) of the TSR defines a “negative option feature” as “an offer or agreement to sell or provide any goods or services, a provision under which the customer’s silence or failure to take an affirmative action to reject goods or services or to cancel the agreement is interpreted by the seller as acceptance of the offer.”

58. Section 310.3(a)(1) of the TSR prohibits any seller or telemarketer from failing to disclose clearly and conspicuously and prior to a consumer consenting to pay for goods or services offered, the following material information:

- a. The total costs to purchase, receive, or use, and the quantity of goods or services that are the subject of the sales offer, 16 C.F.R. § 310.3(a)(1)(i);

- b. All material restrictions, limitations, or conditions to purchase, receive, or use the goods or services that are the subject of the sales offer, 16 C.F.R. § 310.3(a)(1)(ii);
- c. If the seller has a policy of not making refunds, cancellations, exchanges, or repurchases, a statement informing the customer that this is the seller's policy; or, if the seller or telemarketer makes a representation about a refund, cancellation, exchange, or repurchase policy, a statement of all material terms and conditions of such policy, 16 C.F.R. § 310.3(a)(1)(iii); and
- d. If the offer includes a negative option feature, all material terms of the negative option feature, including but not limited to the fact that the customer's account will be charged unless the customer takes an affirmative action to avoid the charge(s), the date(s) the charge(s) will be submitted for payment, and the specific steps the customer must take to avoid the charge(s). 16 C.F.R. § 310.3(a)(1)(vii).

59. Section 310.3(a)(4) of the TSR prohibits any seller or telemarketer from making a false or misleading statement to induce any person to pay for goods or services.

60. Pursuant to Section 3(c) of the Telemarketing Act, 15 U.S.C. § 6102(c) and Section 18(d)(3) of the FTC Act, 15 U.S.C. § 57a(d)(3), a violation of the TSR constitutes an unfair or deceptive act or practice in or affecting commerce, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

COUNT III

Deceptive Telemarketing Calls in Violation of the TSR

61. In numerous instances, in the course of telemarketing their goods and services, Defendants have made false or misleading statements, directly or by implication, to induce consumers to pay for goods or services, including, but not limited to, misrepresentations that

- a. they have detected viruses and infections on consumers' computers that affect the security of consumers' computers and prevent access to consumers' email and other accounts; and
 - b. they are part of, affiliated with, or authorized to provide services for well-known U.S. technology companies.
62. Defendants' acts or practices, as described in Paragraph 61 above, are deceptive telemarketing acts or practices that violate the TSR, 16 C.F.R. §§ 310.3(a)(4), 310.6(b)(4).

COUNT IV
Failure to Clearly and Conspicuously Disclose Material Terms

63. In numerous instances, in the course of telemarketing their goods and services, Defendants have failed to disclose clearly and conspicuously and prior to a consumer consenting to pay for goods or services offered:

- a. The total costs to purchase, receive, or use the goods or services that are the subject of the sales offer;
- b. All material restrictions, limitations, or conditions to purchase, receive, or use the goods or services that are the subject of the sales offer;
- c. That the seller does not provide any refunds;
- d. All material terms and conditions of a negative option feature, including that:
 - i. the consumer's account will be subject to a fixed continuing monthly charge unless the consumer takes affirmative steps to avoid the charge;
 - ii. the date the charge will be submitted for payment;
 - iii. a consumer who agrees to ongoing technical support service plans for a monthly fee is enrolled for 12 months, and automatically renewed for each

subsequent year unless he or she cancels by written letter at least 30 days prior the end of the 12 month term; and

- iv. if the consumer cancels the service within the first 12 month term, he or she will have to pay a \$150 cancellation fee.

64. Defendants' failure to disclose, or to disclose clearly and conspicuously, the information set forth in Paragraph 63 constitutes a deceptive telemarketing act or practice in violation of Section 310.3(a)(1).

VIOLATIONS OF RESTORE ONLINE SHOPPERS' CONFIDENCE ACT

65. In 2010, Congress passed the Restore Online Shoppers' Confidence Act, 15 U.S.C. §§ 8401 et seq., which became effective on December 29, 2010. Congress passed ROSCA because "[c]onsumer confidence is essential to the growth of online commerce. To continue its development as a marketplace, the Internet must provide consumers with clear, accurate information and give sellers an opportunity to fairly compete with one another for consumers' business." Section 2 of ROSCA, 15 U.S.C. § 8401.

66. Section 4 of ROSCA, 15 U.S.C. § 8403, generally prohibits charging consumers for goods or services sold in transactions effected on the Internet through a negative option feature, as that term is defined in the Commission's Telemarketing Sales Rule ("TSR"), 16 C.F.R. § 310.2(w), unless the seller (1) provides text that clearly and conspicuously discloses all material terms of the transaction before obtaining the consumer's billing information, (2) obtains the consumer's express informed consent before making the charge, and (3) provides a simple mechanism to stop recurring charges. 15 U.S.C. § 8403.

67. As described in Paragraphs 34 to 40 above, Defendants have advertised and sold technical support service plans through a negative option feature defined by the TSR. 16 C.F.R. § 310.2(w).

68. Pursuant to Section 5 of ROSCA, 15 U.S.C. § 8404, a violation of ROSCA is a violation of a rule promulgated under Section 18 of the FTC Act, 15 U.S.C. § 57a.

COUNT V
Illegal Negative Option Marketing

69. In numerous instances, in connection with charging consumers for technical support service plans sold in transactions effected on the Internet through a negative option feature, Defendants have failed to:

- a. Provide text that clearly and conspicuously discloses all material terms of the transactions before obtaining consumers' billing information, including: (i) the total cost of the transactions; (ii) that Defendants automatically enroll consumers in a negative option plan for one year at a monthly fee; (iii) that consumers must affirmatively cancel the plan by written letter at least 30 days before the end of the 12-month term to avoid automatic renewal and future charges; and (iv) that consumers who cancel within the first 12-month term will be subject to a \$150 cancellation fee;
- b. Obtain consumers' express informed consent before charging the consumers' credit cards, debit cards, bank accounts, or other financial accounts for products or services through such transactions; and
- c. Provide a simple mechanism for a consumer to stop recurring charges from being placed on the consumer's credit card, debit card, bank account, or other financial account.

70. Defendants' acts or practices, as described in Paragraph 69, above, violate Section 4 of ROSCA, 15 U.S.C. § 8403.

CONSUMER INJURY

71. Consumers have suffered and will continue to suffer substantial injury as a result of Defendants' violations of the FTC Act, the TSR, and ROSCA. In addition, Defendants have been unjustly enriched as a result of their unlawful acts or practices. Absent injunctive relief by this Court, Defendants are likely to continue to injure consumers, reap unjust enrichment, and harm the public interest.

THIS COURT'S POWER TO GRANT RELIEF

72. Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), empowers this Court to grant injunctive and such other relief as the Court may deem appropriate to halt and redress violations of any provision of law enforced by the FTC. The Court, in the exercise of its equitable jurisdiction, may award ancillary relief, including rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies, to prevent and remedy any violation of any provision of law enforced by the FTC.

73. Section 19 of the FTC Act, 15 U.S.C. § 57b, and Section 6(b) of the Telemarketing Act, 15 U.S.C. § 6105(b), authorize this Court to grant such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the TSR, including the rescission or reformation of contracts, and the refund of money.

PRAYER FOR RELIEF

Wherefore, Plaintiff FTC, pursuant to Sections 13(b) and 19 of the FTC Act, 15 U.S.C. §§ 53(b) and 57b, the TSR, and the Court's own equitable powers, request that the Court:

A. Award Plaintiff such preliminary injunctive and ancillary relief as may be necessary to avert the likelihood of consumer injury during the pendency of this action and to preserve the possibility of effective final relief, including but not limited to temporary and preliminary injunctions, and an order providing for immediate access, the turnover of business records, an asset freeze, the appointment of a receiver, and the disruption of domain and telephone services;

B. Enter a permanent injunction to prevent future violations of the FTC Act, the TSR, and ROSCA by Defendants;

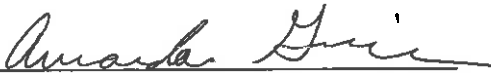
C. Award such relief as the Court finds necessary to redress injury to consumers resulting from Defendants' violations of the FTC Act, the TSR, and ROSCA, including but not limited to, rescission or reformation of contracts, restitution, the refund of monies paid, and the disgorgement of ill-gotten monies; and

D. Award Plaintiff FTC the costs of bringing this action, as well as such other and additional relief as the Court may determine to be just and proper.

Respectfully submitted,

ALDEN F. ABBOTT
General Counsel

Dated: February 25, 2019


Amanda Grier
Colleen B. Robbins
Elsie B. Kappler
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-3845; agrier@ftc.gov
(202) 326-2548; crobbins@ftc.gov
(202) 326-2466; ekappler@ftc.gov
Attorneys for Plaintiff
FEDERAL TRADE COMMISSION